Kryptographie Blatt 7

hhu Düsseldorf
WiSe 2023/24

Abgabe: bis Montag 04.12.2023, vor der Vorlesung

Vorlesungswebseite: `http://reh.math.uni-duesseldorf.de/~khalupczok/krypto/`

Aufgabe 1: Zur Miller–Rabin-Bedingung

(a) Berechnen Sie alle Quadratwurzeln von 1 und -1 mod $n = 2 \cdot 13 \cdot 17 = 442$.

(b) Sei $n = 257$ und $a = 17$. Dann ist $\varphi(n) = 256 = 2^8 =: 2^s \cdot d$ mit $2 \nmid d$, d. h. $s = 8$ und $d = 1$. Berechnen Sie das kleinste $k \in \mathbb{N}$ mit $(a^d)^{2^k} \equiv -1 \bmod n$. Warum gibt es ein solches k nicht, wenn $n = 221 = 13 \cdot 17$ ist?

Aufgabe 2: Wahrscheinlichkeit für die Wahl ganzer Zahlen mod n gewisser Ordnungen

Sei $n = p_1 \dots p_k$ mit paarweise verschiedenen Primfaktoren $p_1, \dots, p_k > 2$ und $2^{s_i} \| p_i - 1$ mit $s_1 \le s_2 \le \dots \le s_k$. Sei P_n die Wahrscheinlichkeit, dass ein beliebiges $y \in \mathbb{Z}_n^\times$ eine gerade Ordnung r besitzt, für die $y^{r/2} \not\equiv -1 \bmod n$ gilt. Zeigen Sie, dass

$$P_n = 1 - 2^{-(s_1 + \dots + s_k)} \Big(1 + \frac{2^{s_1 k} - 1}{2^k - 1}\Big)$$

gilt, und dass dieser Ausdruck $\ge 1 - 2^{1-k}$ ist.

Aufgabe 3: Rechnen im AES-Körper

Gegeben ist der AES-Körper $F = \mathbb{F}_{2^8} := \mathbb{Z}_2[X]/(f)$ mit dem irreduziblen Polynom $f(X) := X^8 + X^4 + X^3 + X + 1$. Ist α die Restklasse von X in F, so schreibt man die Elemente von F als

$$(*) \qquad b_7\alpha^7 + b_6\alpha^6 + \dots + b_1\alpha + b_0$$

mit $b_i \in \mathbb{Z}_2 = \{0, 1\}$. Beim Rechnen mit diesen Elementen kann man α^8 stets auf $\alpha^8 = \alpha^4 + \alpha^3 + \alpha + 1$ reduzieren. Die Koeffizienten werden als **Byte** $b_7 b_6 \dots b_1 b_0$ abgekürzt und als Zahlen im Dualsystem aufgefasst. Beim Umrechnen in das Hexadezimalsystem (Basis 16) werden diese dann mit zwei Hexadezimalziffern (`0,1,2,...,9,A,B,C,D,E,F`) dargestellt, z. B. $1 =$`01`, $\alpha =$`02`, $\alpha + 1 =$`03`, $\alpha^2 =$`04` usw.

(a) Geben Sie die Darstellung von `05`, …, `10` in der Form (*) an.

(b) Berechnen Sie `10`$\cdot$`09`, α^{16}, α^{32}, `9A`$\cdot$`0C` als Hexadezimalzahl.